eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Auditando Senhas:**
  - ✓ Definição de Senha
  - ✓ Ataques não eletrônicos
  - ✓ Ataques Offline
    - ✓ Cluster
    - ✓ Modalidades
    - ✓ Hashes Comunitárias
    - ✓ Tipos
    - ✓ Ferramentas
  - ✓ Ataques Online
    - ✓ Ferramentas
  - ✓ Ataques Passivos
    - ✓ Ferramentas

Advanced Brute Force

eSecurity

www.eSecurity.com.br

Definição de Senha

Uma senha (português brasileiro) ou palavra-passe (português europeu), ou ainda palavra-chave ou password, é uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento.

Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo — ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

Existem diversas formas de realizar ataques à sistemas com senhas. Durante esta aula, iremos tipificar e exemplificar cada uma delas:

Tipos de Ataques:

- Ataques não eletrônicos
- Ataques offline
- Ataques online
- Ataques passivos

Ataques Não Eletrônicos

É possível realizar a coleta de senhas utilizando métodos não eletrônicos, esses métodos são fáceis e muitas vezes, explora a vulnerabilidade humana.

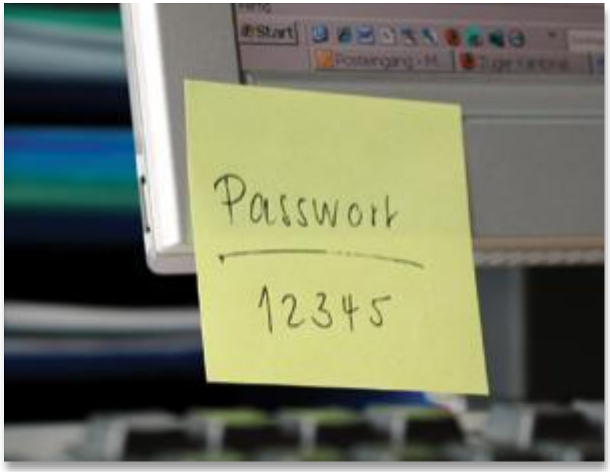
Tais como:

1. Engenharia Social - Induzir alguém a fornecer a senha. Na maioria dos casos, involuntariamente.

2. Dumpster Diving – Encontrar a senha descartada no Linux

3. Shoulder Surfing – Coletar a senha, observando a digitação alheia.

4. Ingenuidade – Capturar senhas anotadas em postits, cadernos, papel, celulares, etc



Ataques Offline

Os ataques off-line consistem em capturar as hashes e tentar efetuar a quebra de modo que o alvo não perceba e não gere ruídos.

Ao realizar o ataque local, você também terá um desempenho muito maior do que o ataques online, isso porque você não irá necessitar de link de rede, internet ou afins.

É possível amplificar o ataque utilizando a GPU de uma placa de vídeo, visto que ela possui um nível de processamento mais rápido.

Pode-se também, ampliar mais ainda fazendo com que essas senhas sejam quebradas em cluster.

Ataques Offline: Cluster

Ataques Offline: Cluster

Ataques Offline: Cluster

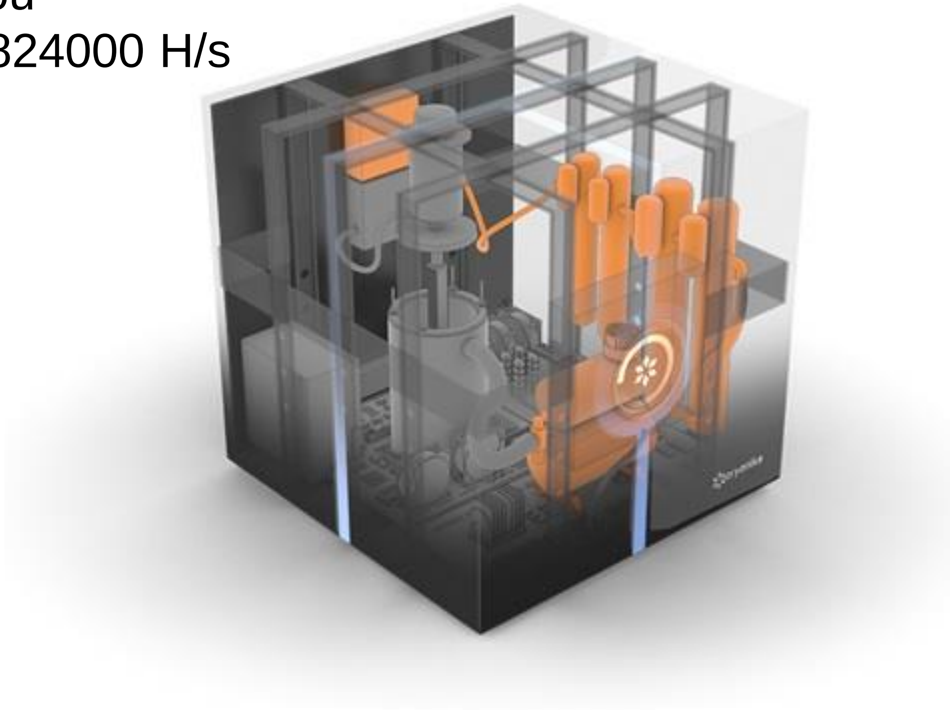
Ataques Offline: Cluster

Ataques Offline: Cluster

Ataques Offline: Cluster

Ataques Offline: Cluster

$ 16k
1000 GH/s
ou
1073741824000 H/s



Ataques Offline: Modalidades

Há duas modalidades para quebras de senhas off-line, são elas:

Conversão de senha para hash – Nesta modalidade o atacante converte uma lista de senhas em hashes e faz um check para verificar se coincide com a hash desejada. Esse processo demora mais, afinal, você fará a conversão e também o check.

Exemplo:
Converto a senha xyz para hash MD5, depois comparo com a hash MD5 que tenho.

Conversão de hash para senha – Nesta modalidade você já possui uma wordlist convertida em hashes, sendo assim, é necessário apenas fazer a comparação.

Exemplo:
Crio um banco de dados só de Hashes + Senhas e comparo as Hashes posteriormente.

Ataques Offline: Hashes Comunitárias

Pode-se também utiliza bancos de dados comunitários, alimentados por usuários diariamente.

Esse banco de dados poderá resolver em segundos o que um brute force levaria semanas.

Exemplos:
https://crackstation.net/

http://www.hashkiller.co.uk/

Ataques Offline: Tipos

Além das modalidades, também podemos encontrar alguns tipos diferentes de ataques.

São eles:

Força bruta: Gera-se muitas tentativas para descobrir uma senha ou uma hash

Dicionário: Baseado em uma lista de palavras, é utilizada para checar se a senha está dentre a lista fornecida.

Híbrido: É a mistura entre a Força Bruta e o ataque com dicinário, você pode variar as senha e adicionar caracteres a elas. Ex: helicoptero1, helicoptero2, ...

Rainbow Tables: Procura o hash alvo em uma tabela ou banco de dados e, caso a encontre, retorna a senha correspondente.

Ataques Offline: Ferramentas

Existem diversas ferramentas para realizar a quebra de senhas off-line, dentre elas estão as mais conhecidas, destacadas na listagem abaixo:

- Hash-identifier
- Multiforcer
- Pwdump
- Sucrack
- John the ripper
- Truecrack
- Hashcat

Ataques Online

Os ataques ativos são realizados com a interação com o alvo, seja ele na rede ou na internet.
Essa interatividade gera muito ruído e é de fácil percepção pelo alvo.

Existem diversas modalidades para realização desse tipo de ataque, são elas:

Brute Force – Ao qual você irá realizar quase na sua totalidade os ataques apresentados no modo off-line com a dificuldade de ser online, mais lento e barulhento.
Padronização – Checar se o alvo está utilizando senhas simples ou padrão de sistema.
Malware – Realiza a instalação de um malware para capturar a senha no cache ou durante a digitação (Keylogger)
Injeção de SQL – Injetar um SQL básico afins de enganar o código.

Ataques Online: Ferramentas

Existem diversas ferramentas para realizar a quebra de senhas online, dentre elas estão as mais conhecidas, destacadas na listagem abaixo:

- Brutus
- Hydra
- Medusa
- Pptp-Bruter

Ataques Passivos

Os ataques passivos são mais difíceis de serem detectados, pois, capturam as senhas que "passam" pela rede.
Na maioria dos casos, é falha do serviço que não possui criptografia e transmite senhas de modo clear text.
Também dependerá do usuário realizar o envio da senha, sendo assim, será imensurável o tempo ao qual conseguirá coletar a senha.

As técnicas utilizadas para esse ataque são:

Man in the middle: Captura a senha fechando um canal entre o cliente e o servidor.

Wire Sniffing: Captura senhas trafegadas sem criptografia na rede

Replay: Fornece o hash capturado ao servidor, mesmo sem saber a senha original

Ataques Passivos: Ferramentas

Existem diversas ferramentas para realizar a captura de senhas, dentre elas estão as mais conhecidas, destacadas na listagem abaixo:

- Dsniff
- TcpDump
- Wireshark
- Cain & Abel
- Ettercap

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker